Docket No.: 7368 US0

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Antonio Bovo et al.

Application No.: 10/622,657 | Confirmation No.: 3846

Filed: July 18, 2003 | Art Unit: 2434

For: COMMUNICATION MONITORING IN A MOBILE RADIO NETWORK | Examiner: Jason Kai Yin Gee

SECOND APPEAL BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This is an appeal from the Examiner's final rejection of the above-identified application as set forth in the Final Office Action dated October 9, 2008 ("Second Final Action"). Appellants previously filed an Appeal Brief dated July 31, 2008 ("First Appeal Brief"). Instead of issuing an Examiner's Answer, prosecution has been reopened with a new Final Action that asserts substantially the same rejections as used previous Actions but with a slightly more detailed description of the cited Takagi reference. The additional discussion of the Takagi reference fails to overcome Appellant's previous arguments, which are set forth below in addition to further arguments highlighting claim elements that are missing from the cited references.

Appellants respectfully request a one (1) month extension of time. Please charge any fee for the extension of time to Deposit Account 50-1065.

Appellants request that the Office apply the previously paid Notice of Appeal fee and Appeal Brief fee to the fees due for the present Second Appeal Brief. Due to fee increases since the First Appeal Brief was filed, an additional $30.00 fee is due for both the Notice of Appeal fee and Appeal Brief fee ($60.00 total). See, M.P.E.P. § 1204.01. Please charge the additional fees to Deposit Account 50-1065.

This brief contains items under the following headings as required by 37 C.F.R. § 41.37(c) and M.P.E.P. § 1205.02:

I. REAL PARTY IN INTEREST

The real party in interest for this appeal is:

Tektronix, Inc., an Oregon corporation, which is a subsidiary of Danaher Corporation, a Delaware corporation.

II. RELATED APPEALS AND INTERFERENCES

There are no prior and pending appeals, interferences or judicial proceedings known to Appellants, Appellants' legal representative or assignee which may be related to, directly affect or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

A. Total Number of Claims in Application

Claims 1-14 are pending in the application and stand finally rejected under 35 U.S.C. § 103.

B. Current Status of Claims

1. Claims canceled: None
2. Claims withdrawn from consideration but not canceled: None.
3. Claims pending: 1 - 14.
4. Claims allowed: None.
5. Claims rejected: 1 - 14.

C. Claims On Appeal

The claims on appeal are claims 1 - 14.

IV. STATUS OF AMENDMENTS

No amendments have been submitted by Appellants after the Examiner's final rejection.

V. SUMMARY OF CLAIMED SUBJECT MATTER

A summary of the claimed subject matter is provided, with reference to page numbers and line numbers. Numbers in bold provided in the following description refer to the item numbers identified in the figures.

Independent claim 1 is an apparatus claim related to a system for communications monitoring in a mobile radio network (see Figure 1). The communications monitoring system corresponds to the deciphering device **30**, which comprises three different types of components: a processing device **32**, a deciphering parameter providing device **34**, and a deciphered data providing device **36**. (see page 10, line 16 through page 12, line 9, which corresponds to paragraphs [0022] through [0023] of the Published Application 2004/0057392). The processing device **32** is coupled to multiple links **22** and **24** in the mobile radio network. The processing device determines from data transferred via the multiple links **22** and **24** deciphering parameters, and deciphers the data using the current deciphering parameters to produce deciphered data. The deciphering parameter providing device **34** is coupled to the processing device **32a** in which the current deciphering parameters are filed by the processing device to be available for another processing device **32b** upon request. As shown in Figure 1, there are two processing devices **32a** and **32b** both

connected to deciphering parameter providing device **34**. The deciphered data providing device **36** is coupled to the processing device **32** for providing the deciphered data to an output for protocol analysis, or procedure trace to be performed on the deciphered data. The processing device **32**, the deciphering parameter providing device **34** and the deciphered data providing device **36** are distributed over different locations and are coupled together by a communication link (see Fig. 1 and page 10, line 16 through page 12, line 9, which correspond to paragraphs [0022] through [0023] of the Published Application 2004/0057392).

Independent claim 8 is a method claim for a method of communication monitoring in a mobile network. The method comprises the steps of determining in a processing device **32** from data transferred via multiple links of the mobile radio network coupled to the processing device current deciphering parameters (see step **125**) (see, Fig. 2 and page 10, line 16 through page 12, line 9, which correspond to paragraphs [0022] through [0023] of the Published Application 2004/0057392). Then, deciphering in the processing device the data using the current deciphering parameters to produce deciphered data (see step **180**) (see Fig. 2 and page 10, line 16 through page 12, line 9, which correspond to paragraphs [0022] through [0023] ofthe Published Application 2004/0057392). The processing device **32** files the current deciphering parameters in a deciphering parameter providing device **34** coupled to the processing device so that the current deciphering parameters are available for another processing device upon request (see step **125**) (see, Fig. 1-2 and page 10, line 16 through page 12, line 9, which correspond to paragraphs [0022] through [0023] of the Published Application 2004/0057392). The deciphered data is provided at an output of a deciphered data providing device **36** coupled to the processing device **32**. The deciphered data is used to perform protocol analysis or procedure trace (see page 5, line 21 through page 6, line 9, which corresponds paragraph [0011] of the Published Application). The processing device **32**, deciphering parameter providing device **34**, and deciphered data providing device **36** are distributed over different locations and are coupled together by a communication link (see, Fig. 1 and page 10, line 16 through page 12, line 9, which correspond to paragraphs [0022] through [0023] of the Published Application 2004/0057392).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Whether claims 1-4, 6, 7, 8-11, 13 and 14 are unpatentable under 35 U.S.C. § 103(a) as being obvious based on Takagi *et al.* (U.S. Published Application No. 2001/0047474- hereinafter "Takagi") in view of Malek (U.S. Patent No. 4,920,567 - hereinafter "Malek").

B. Whether claims 5 and 12 are unpatentable under 35 US.C. § 103(a) as being obvious based on Takagi in view of Malek and further in view of Low *et al.* (U.S. Patent No. 6,959,346 - hereinafter "Low").

VII. ARGUMENT

A. Takagi fails to teach or suggest a "deciphering parameter providing device"

Claim 1 requires:

> a deciphering parameter providing device coupled to the processing device in which the current deciphering parameters are filed by the processing device to be available for another processing device upon request.

Claim 8 requires:

> filing by the processing device the current deciphering parameters in a deciphering parameter providing device coupled to the processing device so that the current deciphering parameters are available for another processing device upon request.

The Second Final Action cites Takagi's security server 601 as the claimed "deciphering parameter providing device;" however, security server 601 does not meet the explicit requirements of independent claims 1 or 8.

The independent claims require that current deciphering parameters are **filed into** the deciphering parameter providing device. (*E.g.* "a deciphering parameter providing device . . . **in which** the current deciphering parameters **are filed**" - claim 1; and "**filing** . . . the current deciphering parameters **in** a deciphering parameter providing device" - claim 8). After being filed into the deciphering parameter providing device, the current deciphering parameters must also be "available for another processing device upon request." It is clear from the language of the claims that the current deciphering parameters are not generated by the "deciphering parameter providing device." Instead, as required by the claim language, the "deciphering parameter providing device" receives the current deciphering parameters **from**

the claimed "processing device" during a filing process.

Takagi teaches four schemes for the proper functioning of the TCP-GW. ¶ [0070]-[0075]. In Scheme 4, "the SA information is generated by a security server and provided from the security server to each end point as well as to the proxy if necessary." ¶ [0075]. Paragraph [0098] is cited as teaching that Takagi's security server 601 is the claimed "deciphering parameter providing device." Second Final Action at 4. However, paragraph [0098] actually requires that, in Takagi's scheme 4, "the security server 601 **generates** the IPSec SA information and **gives** the generated IPSec SA information to the terminal 101, the mobile terminal 501 and the TCP-GW 401" (emphasis added).

Takagi does not teach or suggest that the current deciphering parameters are filed into security server 601, as required by claims 1 and 8. Instead, security server 601 is source of the IPSec SA information (i.e. current deciphering parameters), which security server 601 generates on its own. Moreover, Takagi does not teach or suggest that the current deciphering parameters are "filed by the processing device," such as TCP-GW 401, into security server 601. Takagi's security server 601 operates only to generate and transmit IPSec SA information. Security server 601 does not receive or store (i.e. "filed by") current deciphering parameters from TCP-GW 401 or any other device.

Independent claims 1 and 8 require a "deciphering parameter providing device." The Second Final Action cites Takagi as teaching or suggesting such a device; however, as discussed above in detail, Takagi fails to disclose any device having the required features of the claimed deciphering parameter providing device. The Malek and Low references were not cited in the Second Final Action as teaching or suggesting the deciphering parameter providing device and, in fact, those references do not disclose this claim element. Accordingly, the cited references, whether taken alone or in combination, fail to teach or suggest each and every element of independent claims 1 and 8. Therefore, the pending rejection of claims 1 and 8 should be withdrawn and the claims passed to issue.

B. Claims 1-4, 6, 7, 8-11, 13 and 14 are patentable since they are not obvious under 35 USC §103(a)

Claims 1-4,6, 7, 8-11, 13 and 14 were rejected under 35 U.S.C. § 103(a) as being obvious based upon Takagi in view of Malek.

As noted by Appellants in the First Appeal Brief, in KSR International Co. v. Teleflex Inc., 82 USPQ2d 1385 (2007), the United States Supreme Court reiterated that the framework from obvious is provided by Graham v. John Deere (Graham). The factual inquiries enunciated by the Court are as follows:

(A) Determining the scope and content of the prior art;

(B) Ascertaining the differences between the claimed invention and the prior art; and

(C) Resolving the level of ordinary skill in the pertinent art.

(See Examination Guidelines for Determining Obviousness Under 35 US.C. §103 (M.P.E.P. § 2141))

Accordingly, one should first look at the scope and content of Takagi and Malek, and of the combination of the references.

With regard to independent claim 1, the rejection stated that Takagi teaches a system for communication monitoring in a mobile radio network comprising a processing device coupled to multiple links in the mobile radio network (see Fig. 1, processing device gateway 401, 402, 403). Actually, Takagi does not teach a system for communications monitoring. Rather, it relates to a gateway device for carrying out a data relaying at a transport and upper layer between a first terminal device and a second terminal device. Takagi provides for a secure relay to be provided between a mobile terminal 501 and a TCP/IP terminal 101. The TCP GWs (401, 402, 403) that provide this relay are not coupled to multiple links in the mobile radio network, rather each processing device provides a gateway between network 202 and each of networks 203, 204 and 205 that support mobility (see Fig. 1 and paragraphs [0035] - [0036]). A communications monitoring system as shown in Figure 1 of the present application and claimed therein is coupled to multiple links in the mobile radio network, but does not act as an element of the network itself, rather it monitors the network.

The final rejection refers to paragraphs 98, 101 and 102 of Takagi as teaching a deciphering parameter providing device coupled to the processing device, in which the current deciphering parameters are filed by the processing device to be available for another processing device upon request. Paragraph 98, 101 and 102 related to scheme 4 in which the security server 601 generates IPSec SA information and gives the generated IPSec SA information to the terminal 101, and mobile terminal 501 and the TCP-GW 401. This is

separate and distinct from Scheme 3 which is referred to at [0074] and was relied on to support the assertion that the processing device determines current deciphering parameters from the data transferred. Now Scheme 4 and the related teachings are being used to support the assertion that these current deciphering parameters are filed by the processing device. In Takagi two, or more schemes, are being taught. The first in which the parameters are obtained from one end point, and another where they are provided from a storage location security server 601. Takagi does not describe the processing system filing current deciphering parameters in a deciphering parameter providing device, because either the necessary information is provided by an end point (Scheme 3) (see [0074]) or the SA information is generated by the proxy itself (Scheme 4) (see [0075]). Takagi does not describe obtaining parameters from an end point and filing it in the proxy itself or elsewhere. A communications monitoring system, unlike a relay, does participate in the communication directly, but rather monitors the communications. Accordingly, it needs to first discover the deciphering parameter based on the multiple channels that it is coupled to, it can then file these parameters for further use. It cannot itself communicate directly with a server within the network to provide this SA information as contemplated by Takagi.

Next, Takagi is relied upon for teaching a deciphered data providing device coupled to the processing device for providing deciphered data at an output for protocol analysis or procedure trace (referring to paragraph 91). Paragraph 91 provides for an IP input unit to judge whether the TCP relay processing is to be carried out. This is part of the operation of the relay. One of ordinary skill in the art would not understand this as relating to protocol analysis or procedure trace being performed in connection with communication monitoring.

The rejection acknowledges that Takagi does not teach separating the processing device, the deciphering parameter providing device, and the deciphered data providing device and connecting them by a communication link. Malek is relied upon for providing this feature. Malek does not relate to communication monitoring, but rather provides for a secure telephone terminal. Appellants do not understand how the fact that a telephone network uses a communication link to convey a secure communication, relates to a communication monitoring system conveying deciphering parameters to separated components using a communications link.

The rejection states that it would have been obvious to one of ordinary skill in the art

to combine the teachings of Takagi and Malek as they are both directed toward secure communications in a mobile radio network. However, there references do not related to communications monitoring, protocol analysis or procedure trace, and would not provide all of the elements of the present invention. The rejection further states that one of ordinary skill would have been motivated to separate the output unit from the deciphering unit as to allow physical components to be more specialized. However, no source of this is provided. Takagi, Malek or their combination do not teach this separation.

As the rejection has failed to provide a prima facie case to support the rejection under § 103(a), Appellants respectfully request reversal of the rejection of claim 1, and requests allowance of independent claim 1, along with dependent claims 2-7, which depend directly or indirectly from allowable independent claim 1.

With regard to independent claim 8, which is a method claim having similar subject matter to apparatus claim 1, the rejection stated that the method claims were rejected using the same basis of arguments as used in connection with the apparatus claims. The rejection further reiterated that paragraph 91 of Takagi taught performing protocol analysis, or procedure trace on the deciphered data.

For the reasons discussed above in connection with claim 1, Takagi, Malek and their combination fail to provide all of the limitations of claim 8. The cited references fail to one of ordinary skill in the art of communications monitoring with the instruction necessary to combine them to produce the claimed invention, as well as failing to provide any motivation to do so.

Paragraph 91 of Takagi states:

> "[0091] The IP input unit 1423 judges whether the TCP relay processing is to be carried out or not according to the information of the original packet, and gives the packet to the TCP input unit 1405 by judging that the TCP relay processing is to be carried out. The most simple judgment criterion is that all packets are to be relayed by utilizing the TCP connection as long as TCP is used, but it is also possible to use the other attributes such that there are cases of not relaying packets by utilizing the TCP connection even though TCP is used (in which cases the IP relaying will be carried out). This packet is then

> processed according to its content, by the wire .fwdarw. radio relay unit 1407 of the TCP relay unit 1402, the TCP input unit 1405 and the radio TCP output unit 1408."

This describes an operation that allows a relay to process TCP information so that the relay can properly relay the content appropriately. This does not correspond to performing protocol analysis as it would be understood by one of ordinary skill in the art. Protocol analysis as used in the context relates to a process of measurements being made by communications monitoring equipment or systems to assist in assuring the quality operation of the underlying network. Not merely to route content around within the network itself.

As the rejection has failed to provide a prima facie case to support the rejection under § 103(a), Appellants respectfully request reversal of the rejection of claim 8, and request allowance of independent claim 8, along with dependent claims 9-14, which depend directly or indirectly from allowable independent claim 8.

C. Claims 5 and 12 are patentable since they are not obvious under 35 USC §103(a)

Claims 5 and 12 were rejected under 35 U.S.C. § 103(a) as being obvious based on Takagi in view of Malek and further in view of Low.

As noted by Appellants in the First Appeal Brief, column 6, lines 37 - 57, which refers to Figure 4, are cited as teaching that information that is not decrypted remains and waits in the combiner, and the signal is combined with deciphered data once it is determined that the two sets of data correspond to each other. For convenience that section is provided here:

> "Referring to FIG. 4, a simplified flow diagram of a method according to the invention is shown. Here, a packet is received. The master processor inserts a header indicative of classification, cipher processing, combining packets, and providing the combined data to the data output port. The buffer then receives the formatted packet and provides it to a classification processor that strips out classification data within the packet and replaces it with a known classification code. The packet is then returned to the buffer. The returned packet has the classification step removed therefrom either by removing the function from

> the header or by indicating the function as completed. The classified packet is than provided to a processor for ciphering. The cipher processor decrypts the packet data and returns the clear text packer to the buffer. The clear text packet is now provided to a combining processor that detects the packet classification information to determine if it is part of a segmented larger packet and combines it with those segments of the larger packet that are already in the combiner. When the larger packet is complete, it is returned to the buffer and then provided to the output data port."

While there is some mention of the combining processor combining segments of the larger packet with those segments of the larger packet that are already in the combiner after the cipher processor decrypts the packet data, there is nothing to indicate that the combining processor would combine segments of previously unciphered data with decrypted ciphered data to provide. There is nothing to suggest that the packets would be a mix or ciphered and unciphered data, and that any delay would be necessary to allow for recombining these packets. For further insight, please compare Figure 4 of Low with Figure 2 of the present application.

Accordingly, since Low fails to teach this element as suggested in the rejection, and for the reasons given above in connection with the rejection of claims 1 and 8, which claims 5 and 12 depend from respectively, Appellants respectfully request that this rejection be overturned and the application be allowed to issue.

D. Conclusion

For all these reasons, the rejections of claims 1-14 should be reversed as the claims relate to patentable inventions that are not rendered obvious by the cited combination of Takagi, Malek and Low.

Accordingly, Appellants respectfully request that the rejection of claims 1-14 be reversed and that the case be passed on to issuance.

Respectfully submitted,

February 6, 2009
Date

/Michael J. Fogarty, III/
Michael J. Fogarty, III
Attorney for Appellant
Reg. No. 42,541

SLATER & MATSIL, L.L.P.
17950 Preston Rd., Suite 1000
Dallas, Texas 75252
Tel.: 972-732-1001
Fax: 972-732-9218

CLAIMS APPENDIX

1. A system for communication monitoring in a mobile radio network comprising:

a processing device coupled to multiple links in the mobile radio network, the processing device (i) determining from data transferred via the multiple links current deciphering parameters and (ii) deciphering the data using the current deciphering parameters to produce deciphered data;

a deciphering parameter providing device coupled to the processing device in which the current deciphering parameters are filed by the processing device to be available for another processing device upon request;

a deciphered data providing device coupled to the processing device for providing the deciphered data at an output for protocol analysis, or procedure trace to be performed on deciphered data;

wherein the processing device, deciphering parameter providing device and deciphered data providing device are distributed over different locations and are coupled together by a communication link.

2. The system as recited in claim 1 wherein the communication link comprises one selected from the group consisting of a local area network and a wide area network.

3. The system as recited in claim 1 wherein the processing means deciphers data on first ones of the multiple links using an additional deciphering parameter extracted from the data, the data being in the form of packet data units, the additional deciphering parameter being a set of parameters obtained from a subscriber data base entity, from the data flow of the connection, and from each packet data unit as the sequence number of the packet data units.

4. The system as recited in claim 1 where the data includes both unciphered and ciphered data and the processing device comprises:

means for deciphering the ciphered data according to the current deciphering parameters; and

means for combining the unciphered data and the deciphered ciphered data to produce an ordered data flow as the deciphered data.

5. The system as recited in claim 4 wherein the combining means comprises a delay device for delaying the unciphered data while the deciphering means deciphers the ciphered data so the deciphered data is in the ordered data flow with the unciphered data.

6. The system as recited in claim 1 wherein the processing device comprises a memory coupled to the deciphering parameter providing device for storing deciphering parameters provided by the deciphering parameter providing device.

7. The system as recited in claim 1 wherein the processing device comprises a plurality of processors operating in parallel with the deciphering parameter providing device and deciphered data providing device, the number of processors being sufficient to cover all the multiple links at a serving switching entity.

8. A method of communication monitoring in a mobile radio network comprising the steps of:

determining in a processing device from data transferred via multiple links of the mobile radio network coupled to the processing device current deciphering parameters;

deciphering in the processing device the data using the current deciphering parameters to produce deciphered data;

filing by the processing device the current deciphering parameters in a deciphering parameter providing device coupled to the processing device so that the current deciphering parameters are available for another processing device upon request;

providing the deciphered data at an output of a deciphered data providing device coupled to the processing device;

performing protocol analysis, or procedure trace on the deciphered data;

wherein the processing device, deciphering parameter providing device and deciphered data providing device are distributed over different locations and are coupled together by a communication link.

9. The method as recited in claim 8 wherein the communication link comprises one selected from the group consisting of a local area network and a wide area network.

10. The method as recited in claim 8 wherein the deciphering step comprises the step of deciphering data on first ones of the multiple links using an additional deciphering parameter extracted from the data, the data being in the form of packet data units, the additional deciphering parameter being a set of parameters obtained from a subscriber data base entity, from the data flow of the connection, and from each packet data unit as the sequence number of the packet data units.

11. The method as recited in claim 8 where the data includes both unciphered and ciphered data and the deciphering step comprises the steps of:

deciphering the ciphered data according to the current deciphering parameters; and

means for combining the unciphered data and the deciphered ciphered data to produce an ordered data flow as the deciphered data.

12. The method as recited in claim 11 wherein the combining step comprises the step of delaying the unciphered data while the deciphering step deciphers the ciphered data so the deciphered data is in the ordered data flow with the unciphered data.

13. The method as recited in claim 8 wherein the filing step comprises the step of storing deciphering parameters provided by the deciphering parameter providing device in a memory coupled to the deciphering parameter providing device.

14. The method as recited in claim 8 wherein the processing device comprises a plurality of processors operating in parallel with the deciphering parameter providing device and deciphered data providing device, the number of processors being sufficient to cover all the multiple links at a serving switching entity.

EVIDENCE APPENDIX

No evidence was submitted pursuant to §§ 1.130, 1.131, or 1.132 and no other evidence was entered by the Examiner.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings identified in this Brief.